NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PREVENTING POINT-OF-SALE SYSTEM INTRUSIONS

by

David C. Smith

June 2014

Thesis Advisor:	Neil Rowe
Second Reader:	Garrett McGrath

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704–0188*

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2014	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE PREVENTING POINT-OF-SALE SYSTEM INTRUSIONS	**5. FUNDING NUMBERS**
6. AUTHOR(S) David C. Smith	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Several major United States retailers have suffered large-scale thefts of payment card information as the result of intrusions against point-of-sale systems (smart cash registers). Point-of-sale attacks present a growing threat and can constitute a homeland-security problem due to a trans-national cyber crime element. This thesis presents results of a survey of point-of-sale intrusions that reached at least the start of criminal investigation. The survey showed that attacks were generally quite simple, and predominantly involved guessing passwords and subsequent installation of keyboard loggers. That suggests that countermeasures can be relatively simple although they must overcome organizational inertia. Our analysis leads to several recommendations to improve point-of-sale system security.

14. SUBJECT TERMS Point-of-Sale Systems, Cybercrime, Payment Card Systems	**15. NUMBER OF PAGES** 75
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

PREVENTING POINT-OF-SALE SYSTEM INTRUSIONS

David C. Smith
Assistant to the Special Agent in Charge, United States Secret Service
B.A., The University of Michigan, 1989
M.A., The University of Michigan, 1990

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN CYBER SYSTEMS AND OPERATIONS

from the

**NAVAL POSTGRADUATE SCHOOL
June 2014**

Author: David C. Smith

Approved by: Neil Rowe
Thesis Advisor

Garrett McGrath
Second Reader

Cynthia Irvine
Chair, Cyber Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Several major United States retailers have suffered large-scale thefts of payment card information as the result of intrusions against point-of-sale systems (smart cash registers). Point-of-sale attacks present a growing threat and can constitute a homeland-security problem due to a trans-national cyber crime element. This thesis presents results of a survey of point-of-sale intrusions that reached at least the start of criminal investigation. The survey showed that attacks were generally quite simple, and predominantly involved guessing passwords and subsequent installation of keyboard loggers. That suggests that countermeasures can be relatively simple although they must overcome organizational inertia. Our analysis leads to several recommendations to improve point-of-sale system security.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
ATM	automated teller machine
CVV	card verification value
DHS	The Department of Homeland Security
HVAC	heating, ventilating, and air conditioning
IP	Internet Protocol
MAC	Media Access Control
PCAP	packet capture file format
PIN	personal identification number
RAM	random access memory
RDE	remote desktop environment
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USC	United States Code
USSS	United States Secret Service

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank Dr. Neil Rowe for his expert guidance and direction on this project. Dr. Rowe provided valuable support and suggestions, and he skillfully kept me on track when I drifted off course.

I also would like to thank Garrett McGrath for his comments and guidance on this project. This work is much better thanks to his mentorship.

Finally, I would like to thank my colleagues of the United States Secret Service for the tremendous support and encouragement that I received throughout this entire process.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

On December 19, 2013, the Target department store chain, the second-largest retailer in the United States, announced in a press release that hackers had exfiltrated approximately forty million credit and debit-card numbers, from November 27 through December 15, 2013 (Target, 2013). The criminals transferred the stolen data to a server in Russia (Raff, 2014).

Since the initial news, there have been numerous postings and announcements from Target, security blogs, and security research companies regarding the intrusion. Although the specific details are still unfolding as of the writing of this thesis, there has been significant attention focused on Target's point-of-sale terminals, the locations where customers physically swipe their credit or debit cards for payment.

The Target network intrusion, and the subsequent news that the Nieman Marcus retail chain suffered a similar hack (Krebs, 2013; Krebs, 2014, January 10), has brought national attention to point-of-sale systems and the potential for significant fraud due to compromised payment card information. On February 04, 2014, high-level executives from Target and Nieman Marcus prepared written testimonials in advance of several congressional hearings on retail data breaches the week of February 05, 2014 (Associated Press, 2014; United States Senate, 2014).

While the Target data breach attracted significant national attention due to the magnitude of the data losses, the compromise of credit and debit card numbers due to network intrusions of point-of-sale systems has been a problem for several years. Trustwave, an incident response and security research company, identified point-of-sale system malware as far back as July 2008 (Percoco, Sheppard, & Ilyas, n.d.). Much of the discussion among Congress, the Federal Trade Commission, the retail industry, and security experts has focused on two areas: whether the United States should move to the chip-and-personal identification number (PIN) system used in other parts of the world, and whether Congress should pass a federal data breach notification law that would require businesses to notify customers if card data had been compromised (Hans, 2014).

These two suggestions—a Chip-and-PIN system and a federal data breach law—will do nothing to address the question of why hackers so easily breach point-of-sale systems. Chip-and-PIN systems will make it more difficult for criminals to manufacture counterfeit payment cards, and therefore may remove some of the incentive for criminals to attempt point-of-sale system intrusions, but moving to such a system will not prevent point-of-sale intrusions themselves. Although law enforcement agents and forensic specialists are still investigating the Target intrusion, the latest public information suggests that hackers infiltrated the Target network using network credentials stolen from a company contracted by Target to manage the latter's climate control (HVAC) systems (Krebs, 2014 February 6).

A. PROBLEM STATEMENT

Congressional testimony concerning the recent data breaches against Target and Neiman Marcus has brought much needed focus and attention on the problem of payment card security throughout the retail industry (Douglas, 2014). Members of Congress and corporate executives have suggested migrating toward a more secure PIN-and-Chip card system and passing Federal legislation concerning data breach notifications and consumer protection (Associated Press, 2014). Data-breach notification laws have their own intrinsic value, but if stronger information security practices reduce the number and impact of point-of-sale system intrusions, there will be less of a need for data-breach notification laws.

B. PURPOSE OF STUDY

The Department of Homeland Security, in its *Quadrennial Homeland Security Review Report*, listed several departmental goals (Department of Homeland Security, 2010). Among these are "Create a Safe, Secure, and

Resilient Cyber Environment" and "Promote Cybersecurity Knowledge and Innovation". Within the Department of Homeland Security, the United States Secret Service shares jurisdictional authority to investigate network intrusions against point-of-sale systems (18 U.S. Code § 1030). The U.S. Secret Service works closely with private forensics firms and other law enforcement agencies to develop forensic knowledge and techniques related to point-of-sale system breaches. By analyzing criminal investigations into point-of-sale systems, this information will equip the Department of Homeland Security to improve public awareness efforts toward securing point-of-sale systems. We have an additional goal of advancing the discussion of and research into forensic tools and techniques in support of point-of-sale system criminal investigations.

C. LIMITATIONS

In conducting research and analysis on the subject of point-of-sale system data breaches, we encountered several limitations:

- There were no reliable statistics regarding how many criminal intrusions have taken place targeting retail point-of-sale systems. For similar reasons, there are no specific data regarding actual fraud losses to financial institutions, retail establishments, and consumers.
- To protect the integrity of active investigations and the privacy of victims, only aggregated data will be discussed. Specific case studies will be limited to those with publicly released judicial documents.
- In some cases used to supply the aggregate data, specific items such as the name and characteristics of malware used were not available. In some cases, for example, the victim or point-of-sale system vendor performed a cleanup of the system thus eliminating evidence.

D. METHODOLOGY

This thesis will evaluate several notable point-of-sale data breaches based on publicly available information, including publicized attacks against the Subway sandwich chain and the recent theft of card data from Target and Neiman

Marcus. It will examine open-source documents illustrating the trans-national criminal element of online card data compromises. Finally, it will reference a variety of data breach studies, both point-of-sale-specific and not, from major forensic firms including Trustwave and Verizon.

To develop insight into individual data breaches, this thesis examined forty-two active and recently closed criminal investigations by agents of the U.S. Secret Service. Our goal in performing these case studies was to determine if there were specific trends related to the nature of the point-of-sale system intrusion (i.e., how did the hackers break in), the hacking exploits or malicious code used, the duration of the attacks, and how the intrusion was discovered.

Finally, as a model for a potential mitigation strategy for the problem of point-of-sale system intrusions, the thesis gives specific recommendations for securing systems and maintaining good security practices. It also reviews an ongoing successful federal crime-prevention program that may serve as a model for a similar effort to reduce point-of-sale system intrusions through public education.

II. REVIEW OF LITERATURE

Point-of-sale systems typically include one or more terminals, a back-of-house server, and a connection to the Internet or to a corporate network. The terminals usually consist of a standalone card terminal (common in supermarkets and department stores, for example) connected to a computer, or a card terminal connected to a touch-screen monitor (common in restaurants and bars, for example). These terminals read the track data from cards and forward the information to a back-of-house server. The back-of-house server collects card data from the merchant’s terminals and relays it to a payment processor for card approval or denial. Larger corporations may use a different configuration in which card data is sent through a corporate office before it reaches a payment processor. Point-of-sale systems include card reading hardware (i.e., the terminals) and software to read data and forward the data to card processors. Most point-of-sale systems for small and medium-sized businesses use standard Microsoft Windows desktops to run the terminals, and use a Windows server as the platform for the back-of-house server. Figure 1 illustrates two common point-of-sale system topologies, the first for a small business and the second for a larger corporation (Trustwave, 2014).

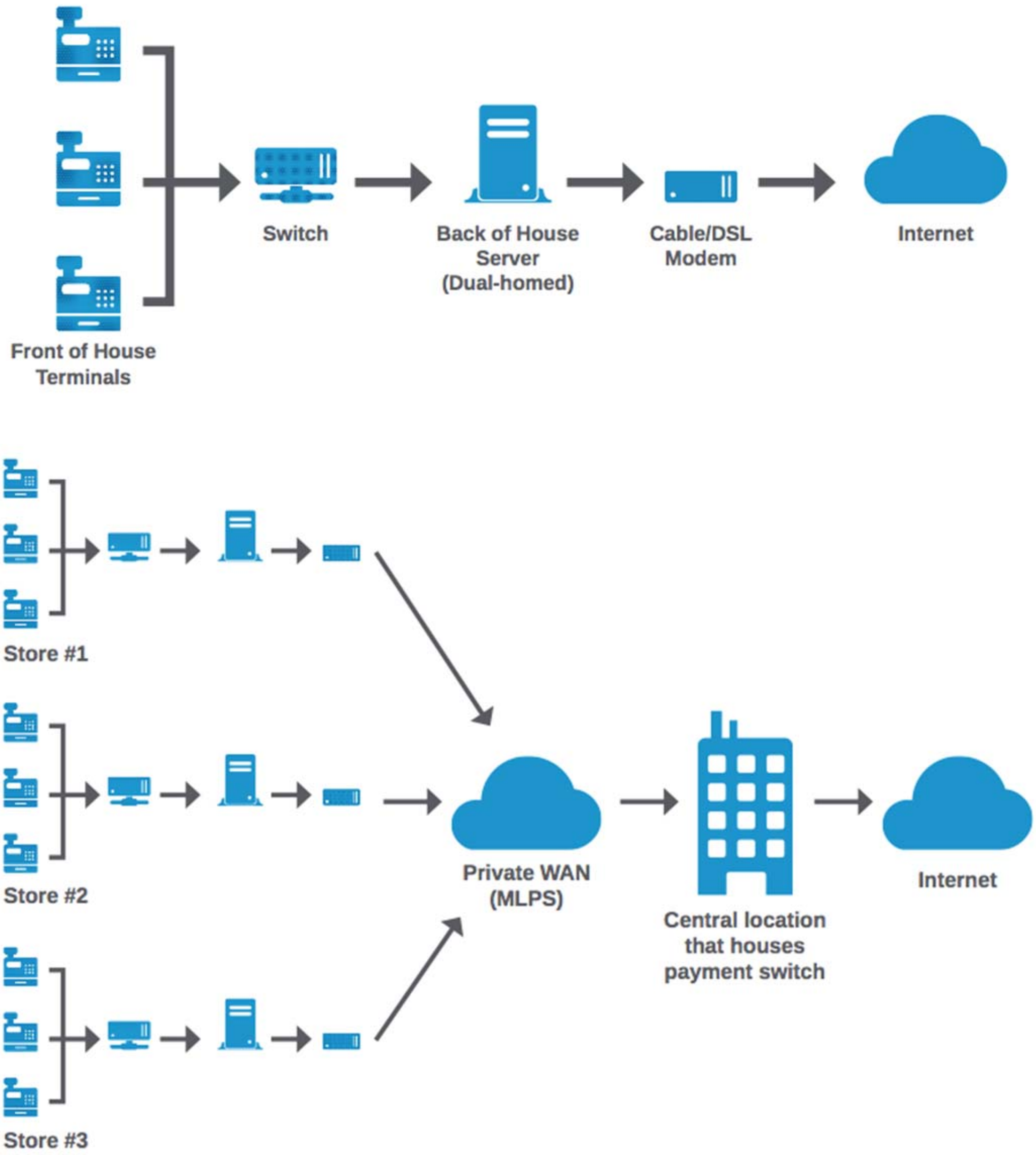

Figure 1. Point-of-Sale System Topologies for Small and Large Merchants

A. POINT OF SALE SYSTEMS AND ATTACKS

Point-of-sale system attacks are new in terms of published books and professional literature, but there has been some prior work assessing specific threats.

Hizver and Chiueh performed an analysis of point-of-sale systems software processes on a Windows server in a virtual environment (Hizver & Chiueh, 2012). The authors showed that once the memory locations of the processes were located, a random access memory tool could simply search for ASCII strings consistent with credit card numbers; that is, 13- or 16-digit strings beginning with certain digits (e.g., a 4 for a Visa or a 5 for a MasterCard). This in fact is the premise behind memory scraping malicious code.

Venter et al describe a suite of malware files that currently exist in the wild including “ramsys32.sys,” a malware controller application known as “loader.exe,” and a dynamic link library called “searcher.dll” (Ventner, Sheppard, & Percoco, 2010). The authors explain how these three malicious files work together to scan for and copy out card track data once such data appears in memory. “Searcher.dll” appears in numerous cases examined in Chapter IV.

Bowles et al. propose a method for exploiting point-of-sale system PIN entry devices (Bowles, Cuthbert, & Stewart, 2005). Their analysis focuses on physical attacks against such devices, as for example inserting a hardware or software sniffer inside the point-of-sale and PIN hardware. The Michaels craft store chain suffered such an attack against their physical point-of-sale and PIN devices in 2011 (Krebs, 2011).

Many small businesses rely on a point-of-sale system vendor to perform technical updates or repairs. In order to provide real-time customer support, especially during non-business hours, some point-of-sale system vendors install a remote desktop environment (RDE) product on the business’s point-of-sale system. Many hackers who target point-of-sale systems begin by gathering a list of common network ports associated with well-known remote desktop products. For example, PC Anywhere typically runs on TCP port 5631 or 65301 for data, and UDP port 22 or 5632 for status transmissions. Hackers will scan IP addresses connected to restaurants or businesses, looking for indications that those ports are open. Port scanning is a long established technique, and the pre-eminent tool for port scanning is Nmap. There are many options available for the Nmap tool (Lyon, 2008).

B. NONVOLATILE FORENSIC ARTIFACTS

For point-of-sale system intrusions, investigators focus on a variety of volatile and non-volatile forensic clues. In general, volatile artifacts are those elements that are in main memory and will disappear if the network connection is lost or if the affected machine is restarted. Non-volatile forensic artifacts are those items that are typically written to disk, such as a file or Windows Registry key. In general, Secret Service best practices call for agents to acquire both kinds of forensic data- if the circumstances of the investigation allow for such collection.

In non-volatile forensic data collection, an important focal point is the Windows Registry, which is a large collection of user and system settings. Many types of malware used in point-of-sale system intrusions leave or modify one or more identifiable keys in the Windows Registry.

Carvey proposes a method for analyzing volatile, semi-volatile, and archived information on Microsoft Windows-based computers (Carvey, 2012). A number of Carvey’s techniques, for example acquiring and analyzing the Windows Registry hives from the live machine, are particularly useful for analyzing compromised Windows based point-of-sale terminals (the terminals where employees place orders and swipe cards for processing) and back-of-house servers (typically a server that transfers card data and approval information between the terminals and external payment networks) (Carvey, 2011). Many forms of malware used in point-of-sale system intrusions leave specific traces in Registry keys, and Carvey’s techniques for Registry hive acquisition and analysis work well with these types of investigations.

The most common approach to malware detection relies on identifying suspicious files by comparing the checksum (many-to-one mapping) of a questionable file against a list of known checksums linked to known malware. Comparing checksums is a simple task that can be performed with a variety of command line or graphical user interface tools. Since most point-of-sale systems use standard commercial software, including underlying operating systems, checksum verification tools can easily be installed and configured on point-of-sale systems to monitor for malicious code with known checksum values. This technique is limited against new (zero-day) exploits for which checksums of the malicious code will not be available.

Ligh et al. propose a number of additional techniques for analyzing files, Windows registry keys, and memory captures for indications of malicious code infection (Ligh et al. 2011). Their analysis of malware-laced documents (e.g., Adobe pdf files, Microsoft Office documents) is beneficial due to the fact that some point-of-sale system users conduct non-business Internet activities (e.g., checking email or browsing Web sites) on point-of-sale terminals, and thus are potential targets for phishing or other forms of social engineering.

C. VOLATILE FORENSIC ARTIFACTS

Common examples of volatile data are the contents of random-access memory (RAM), running processes, and active network information. Information regarding active processes and network information can be obtained from a series of simple command line tools (e.g., the netstat command), but memory (RAM) capture files may include additional information, such as hidden processes and remnants of terminated network data.

Okolica and Peterson propose a method for analyzing Windows based memory samples for information regarding, among other things, running processes (Okolica & Peterson, 2010). Carvey and Ligh demonstrate the value of studying active processes on a potentially infected or compromised Windows machine (Carvey 2012; Ligh et al., 2011). Point-of-sale system malicious code may initiate one or more running processes on the infected system (hidden or not), therefore these techniques may assist investigators.

Hejazi et al describe a method of "application fingerprinting" to extract information beyond string pattern matching and plain text information such as processes (Hejazi, Talki & Debbabi 2009). Furthermore, they explain a method for studying the operating system call stack and stack frame to search for useful information in a memory capture. This method could be useful to look for indications of malicious code not easily identifiable through simple string searches.

Beverly et al explain a method for extracting network packet data from memory samples (Beverly, Garfinkel, & Cardwell, 2011). Their work describes how network packet artifacts, such as Internet Protocol (IP) addresses, can be recovered, even after network connections have been terminated. This technique could prove valuable if stolen card data has recently been exfiltrated (either manually or through an automated process) by possibly yielding IP addresses or Domain Name Service information.

D. NETWORK-BASED ARTIFACTS

A survey done for this thesis will suggest that most point-of-sale system intrusions use fairly simple attack methods and forms of malware. Attacks generally make little or no effort to hide or disguise the file names or process names of their malicious code. Nevertheless, it is useful to study network packet captures of compromised point-of-sale terminals to analyze indications of unauthorized card data transmissions. Furthermore, while most small businesses offer few opportunities for log-file analysis or forensic evaluation of routers and network switches, there are useful methods involving them.

Chappell provides a discussion of Wireshark, the most popular tool for acquiring and analyzing network packets (Chappell, 2012). She suggests several security related scenarios in which network packet captures would be useful for network forensics, such as when an infected machine sends out unauthorized data or attempts to contact a command and control server. In some forms of point-of-sale attacks criminals will establish an automated file transfer protocol (FTP) or simple mail transport protocol (SMTP) service that will automatically send payment-card collection files to an external file server or free Webmail address.

THIS PAGE INTENTIONALLY LEFT BLANK

III. POINT OF SALE SYSTEM BREACHES: A HOMELAND SECURITY PERSPECTIVE

A. PAYMENT CARD SYSTEM COMPROMISES: A HISTORICAL PERSPECTIVE

Despite the significant number of credit and debit-card accounts compromised from the Target point-of-sale system intrusion, it is not the largest payment-card data breach in history. That dubious distinction belongs to Heartland Payment Systems, a payment processing company in New Jersey. In January 2009, Heartland Payment Systems disclosed that hackers had broken into their network and stolen millions of credit-card numbers (Acohido, 2009). In a federal indictment against the three defendants, the United States government declared that hackers had compromised 130 million credit and debit card numbers (U.S. v. Gonzalez). Prior to the Heartland Payment systems breach, the largest card theft targeted TJX, parent company of clothing retailers TJ Maxx and Marshalls. Over an eighteen-month period in 2005 and 2006, hackers infiltrated the TJX point-of-sale network and garnered approximately 94 million account numbers (Berg, Freeman, & Schneider, 2008).

A study by FICO, a company that specializes in financial analytics and credit scores, identified point-of-sale fraud as far back as 2001 (FICO, 2010). In 2005, researchers from the Electronic Warfare Association-Canada published a paper describing physical attack scenarios against magnetic stripe-based point-of-sale system terminals (Bowles, Cuthbert, & Stewart, 2005). In 2008, the incident response company Trustwave published a report indicating that point-of-sale system hackers were shifting tactics away from data at rest attacks (e.g., SQL Injection attacks or “smash and grab” attacks, in which an intruder breaks into a network to steal one or more flat files containing payment-card data) toward data-in-memory attacks. Trustwave reasoned that as fewer organizations stored payment card data, and such data was encrypted from the time of the swipe to the verification at a card processing company, the hackers realized the only real opportunity to obtain unencrypted card data was during the brief period of time when the card data was in plain text in the point-of-sale terminal’s random access memory (Trustwave, 2008). Indeed, “memory scraping,” which refers to the act of capturing card data as it briefly enters an unencrypted state in a point-of-sale terminal’s random access memory, is the attack of choice for hackers who target data in transit. Trustwave identified memory scraping as the dominant method of capturing card data in its most recent analysis of payment-card system compromises, the *2013 Global Security Report* (Percoco et al., 2013).

B. RECENT HIGH-PROFILE POINT-OF-SALE SYSTEM COMPROMISES

On December 19, 2013, the Target department store chain announced in a press release that hackers compromised approximately 40 million credit and debit card numbers in a three-week period (Target, 2013, December 19). Target released another statement the next day assuring its customers that only credit and debit card track data (name, card number, expiration date, and CVV) had been stolen. Target emphasized that PIN codes for debit-card transactions had not been compromised (Target, 2013, December 20). Target added that customers who shopped at their online site (i.e., target.com) were not affected, suggesting that the intruders compromised the point-of-sale system, the mechanism that processes cards for in-store purchases. On January 12, 2014, Target CEO Gregg Steinhafel confirmed that the data breach included malware infections of point-of-sale terminals (Quick, 2014). In February 2014, investigators focused on Fazio, a company Target contracted for HVAC work. In a publicly released statement, Fazio claimed that they were also victims of the Target data breach, and that Fazio followed industry best practices for information security (Fazio, n.d.; Krebs, 2014, February 12).

Less than a month after Target disclosed its large-scale data breach, representatives from the Neiman Marcus retail chain announced that the high-end retailer had also suffered a network intrusion, compromising 1.1 million credit and debit card numbers (D’Innocenzio, 2014). In a statement, Neiman Marcus revealed that their point-of-sale system was compromised over a period of more than three months (Katz, 2014). According to a Reuters report, malware known as a “memory scraper” was used in both the Target and Neiman Marcus attacks (Finkle & Hosenball, 2014).

The exact potential fraud losses for these two data breaches, affecting over forty-one million credit and debit cards, would be difficult to determine, as each cardholder has a distinct credit limit or debit balance. If we use the United States Sentencing Commission standard of $500 loss per card (United States Sentencing Commission, 2013), then the Target and Neiman Marcus breaches alone could yield over twenty billion dollars in fraud.

C. RECENT PUBLIC DISCOURSE OVER POINT-OF-SALE DATA COMPROMISES

Even after fifteen years of publicity surrounding point-of-sale system compromises, including high-profile criminal arrests and major intrusions against TJX and Heartland Payment Systems, the recent Target and Neiman Marcus data breaches generated significant public attention. In February 2014, Congress held hearings on the Target and Neiman Marcus intrusions. The focus of the hearings, based on testimony of retail executives and comments and questions by members of Congress, centered on the discussion of whether and when the United States retail and financial sectors should move from magnetic-stripe cards to PIN-and-chip based cards. While a move to PIN-and-chip cards will make the counterfeiting of credit and debit cards more difficult, it will not prevent point-of-sale system intrusions themselves since it does not affect memory scraping(Associated Press, 2014).

A secondary discourse centers on whether the United States Congress should pass a national data-breach notification law. Such a law would require retailers and financial institutions to notify cardholders when a data breach has occurred. A federal data breach law would supersede the current patchwork of over forty state-level data breach laws. Congress has attempted to pass a federal data-breach notification law several times over the past decade without success, but the recent focus on Target and Neiman Marcus may provide fresh support for such a law (Selyukh, 2014).

What is absent in the flurry of press releases, Congressional hearings, and news interviews is a discussion of why United States retailers and financial institutions continue to suffer point-of-sale system compromises, despite a long and well publicized history of major breaches.

D. SUBWAY – A CASE STUDY

On May 04, 2011, a federal Grand Jury in New Hampshire indicted six individuals, including four Romanian nationals, for hacking into numerous point-of-sale systems. According to the grand jury, the group of hackers broke into point-of-sale systems of over 150 Subway sandwich franchises and fifty other retailers (U.S. v. Oprea et al.). The hacking group ultimately compromised over 100,000 cards, leading to more than $17.5 million in unauthorized charges and remediation expenses (DOJ, 2013).

The grand jury alleged that the group of six hackers broke into Subway and other retail point-of-sale systems over a period of approximately three years, from April 2008 until March 2011. The grand jury identified the following typical sequence of events:

1. The suspects scanned target systems looking for vulnerable remote desktop software (i.e., port scanning for standard ports used by common remote desktop software and services).

2. The suspects breached the point-of-sale systems by using easy-to-guess passwords or password-cracking tools against the remote desktop software.

3. Once the hackers had access to the point-of-sale system, they installed a back-door (specified in the indictment as xp.exe). This tool allowed the suspects to regain entry and introduce additional software tools.

4. The hackers installed a keylogger (not specifically identified in the indictment) that captured card track data.

5. The hackers exfiltrated the stolen card track data to a series of “dump sites” (FTP servers) maintained by the hackers.

6. From overseas locations, the hackers would transfer the stolen card data from the dump sites to a central file server controlled by the hackers.

7. The hackers would “monetize” (i.e., profit) from the theft of stolen card data by either selling the card data in the criminal underground, or by making unauthorized charges against the compromised accounts. In some instances, “the members created phony plastic credit cards by using hardware and software devices (including magnetic stripe readers/writers) to encode blank plastic cards with the stolen credit card data. They then used these encoded plastic cards to make unauthorized charges with various merchants, primarily located throughout Europe (U.S. v. Oprea et al.).”

Since the indictment, three of the six defendants have pled guilty and have been sentenced. Two unnamed suspects have yet to be identified, and one of the named suspects remains at large in Romania.

The Subway case is not the largest in history, nor is it notable for any form of sophisticated malware or hacking techniques. In many ways, though, the Subway case is a classic model of criminal intrusions into point-of-sale systems. The attackers often begin by running a port scan against IP addresses that belong to restaurants and other retailers, looking for port numbers that correspond to remote desktop software or services such as PC Anywhere, Microsoft Remote Desktop, LogMeIn, or GoToMyPC. Remote access software (sometimes known as a remote desktop environment) is common on point-of-sale systems to allow point-of-sale technicians (usually from the company that installed the point-of-sale system) to remotely log in and troubleshoot issues with a business’s point-of-sale system. Unfortunately these common remote-access products use common port numbers, and the point-of-sale merchants often establish common (de-facto default) user-name and password combinations (Trustwave, 2014). When the intruders find remote desktop ports open, they try easy to guess passwords, default passwords, or employ brute-force password cracking methods. Once inside the restaurant's network, the attackers then employ a keystroke logger or memory scraper to capture card track data. The stolen data is then uploaded to an external file server, usually called a "dumps site," where the criminals later aggregate and sort the card data by card type (Visa, MasterCard, American Express) and location of the issuing bank.

It is worth noting that all of the named suspects, including the three that have pled guilty, are from overseas. Moreover, a portion of the fraud occurred in Europe. The Subway case is but a mere example of how cyber crime has rendered international borders less important, at least for the criminals that gain illegal access to retail establishments, compromise thousands or even millions of cards, then use these accounts to make fraudulent purchases or sell them on "dumps sites," where anyone with Internet access can purchase credit or debit card data with which to make counterfeit cards. The transnational element of cybercrime, which is prevalent with point-of-sale breaches, presents a unique attack against the financial health of the United States.

E. THE TRANSNATIONAL ELEMENT IN PAYMENT SYSTEM BREACHES

On August 07, 2009, French police, using information provided by the United States Secret Service, arrested Vladimir Horohorin as he boarded a plane in Nice on his way back to Russia (DOJ, 2010). According to a Grand Jury indictment, Horohorin, also known as "BadB," operated a fully automated "dumps site," dumps.name. A "dumps site" is a Website devoted to the buying and selling of stolen card data (U.S. v. Horohorin). The United States Department of Justice declared that Horohorin ran one of the largest "dumps sites" in the world until his arrest (DOJ, 2012).

On his Website, Horohorin posted two animated videos glorifying the "carder" lifestyle. In his first video, a Russian and an Italian carder are shown enjoying the fruits of their criminal activities while various United States citizens discover that their account balances are empty (Zetter, 2010). In the second video, the Russian hacker is shown accepting a medal from Russian President Vladimir Putin. At the end of the second video, a statement in broken English reads, in part, "we awaiting for new dumps and new incomes, we awaiting you to fight the imperialism of USA. That way we invest U.S. funds in Russian economy and make it grow bigger! (BadB cartoon, n.d.)"

It is impossible to measure the degree to which anti-American sentiment motivates Russian or other international hackers. There is no question, however, that proceeds from card breaches are changing the dynamics of the worldwide underground economy. In the past three years news organizations have published no fewer than three detailed reports about the Romanian town of Ramnicu Valcea, also known as "Hackerville." According to these articles, proceeds from online fraud and hacking have brought sudden and suspicious wealth to a previously poor city of 100,000 citizens (Bhattacharjee, 2011; Bran, 2013; Odobescu, 2014).

It is impossible to determine the exact involvement and extent of foreign criminals in the world of payment system intrusions and fraud. Not all data breaches are reported to law enforcement, and even in the cases that law enforcement investigates, only a small portion of the suspects are identified, let alone prosecuted. Furthermore, payment system breaches generally involve three types of criminal activity:

1. The illegal network or system intrusion into the point of sale system or payment system, which leads to theft of credit and debit card numbers, expiration dates, and in some cases PIN codes and personal information.

2. The trafficking of numbers of credit and debit cards. Most of the buying and selling of bulk quantities of credit and debit card data is done through

Websites variously called “dumps sites,” “carding portals,” or “carding forums.” Some of the more infamous of these were and are Shadow Crew, Carderplanet, Carder.su, and Mazafaka.ru. In general the criminals that steal credit and debit card numbers sell stolen card data to these “carding” or “dumps” sites. While the criminals will often keep a portion of stolen card data for their own personal use, they sell the vast majority to “carding” sites.

3. The street use of stolen credit and debit card numbers. While the first two kinds of criminals can and often do use compromised card data for their own fraudulent purchases, a large portion of the criminal proceeds occurs by selling data to street-level criminals. For credit-card information, the end-user criminals will make fraudulent purchases online or re-encode the compromised information onto counterfeit credit cards to use in person at stores, hotels, etc. For debit-card information, criminals will make fraudulent purchases online, re-encode the data onto counterfeit cards to make in person fraudulent purchases, or use the counterfeit cards to make cash withdrawals at Automated Teller Machines (ATM), an activity known as a “cash out.” In some instances, a criminal organization will produce hundreds or thousands of counterfeit ATM cards, using stolen card data and PIN codes. The criminal organization will recruit “mules,” or accomplices who are willing to use the fraudulent cards at ATM machines around the world. Generally the “mules” keep a portion of the cash withdrawn, and send the remainder to the criminal organizers.

The layered nature of payment system intrusions and subsequent card fraud means that even a relatively simple theft of credit and debit-card numbers from a small restaurant in Idaho may have connections to large scale transnational organized crime. Figure 2 illustrates a common layout for a “carding” criminal enterprise.

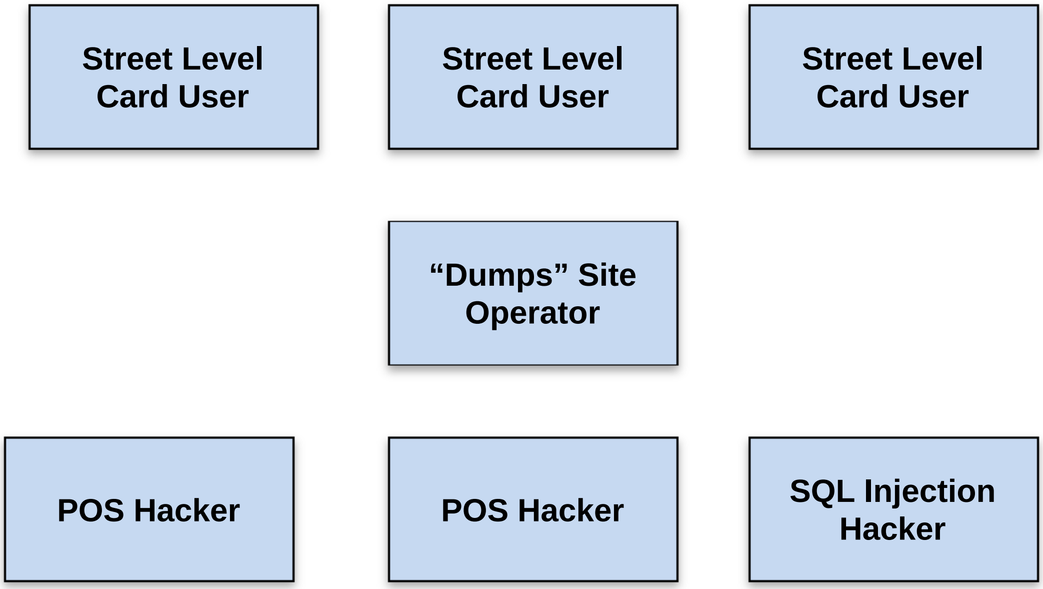

Figure 2. Common Trans-national Criminal Underground "Carding" Hierarchy

The Albert Gonzalez hacking organization provides a good illustration of the trans-national aspect of the criminal "carding" underground. Gonzalez was a hacker involved with the Shadow Crew organization, and later developed his own criminal enterprise. Unlike most carding operations, in which the "dumps" site administrator serves as a pure separator between stolen card sellers (i.e., the POS or other hackers) and buyers (i.e., the street users or "mules"), Gonzalez established and directed all layers of activities. The Gonzalez carding organization included individuals from several countries, thus illustrating the international aspect of the stolen card underground. Figure 3 shows the basic organizational chart of the Gonzalez hacking organization.

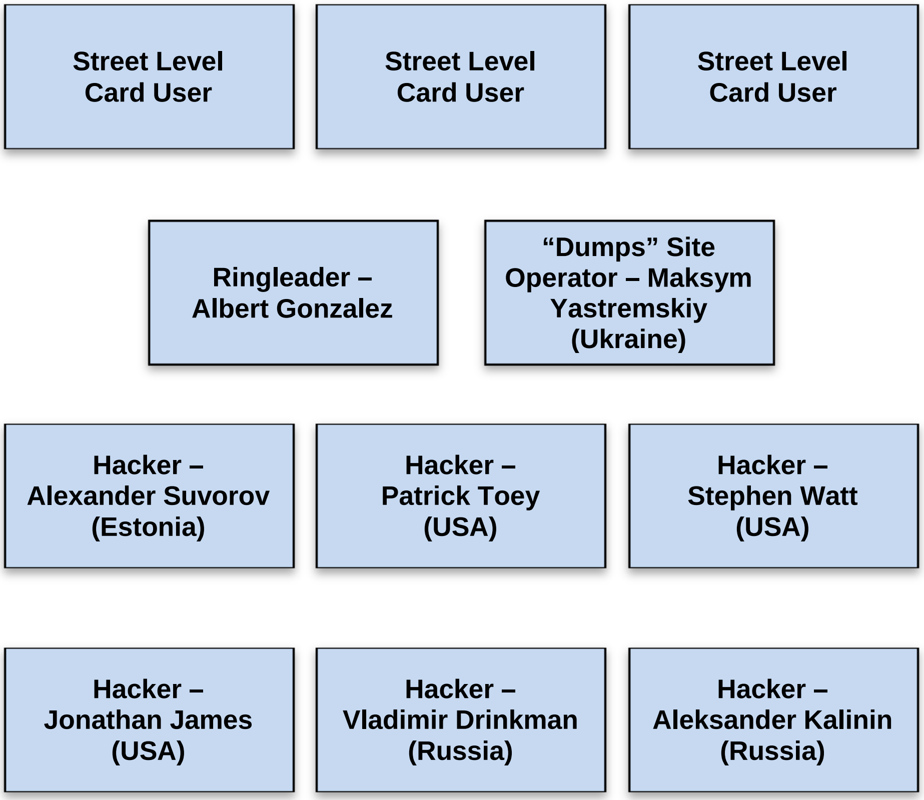
Street Level Card User
Street Level Card User
Street Level Card User
Ringleader – Albert Gonzalez
“Dumps” Site Operator – Maksym Yastremskiy (Ukraine)
Hacker – Alexander Suvorov (Estonia)
Hacker – Patrick Toey (USA)
Hacker – Stephen Watt (USA)
Hacker – Jonathan James (USA)
Hacker – Vladimir Drinkman (Russia)
Hacker – Aleksander Kalinin (Russia)

Figure 3. The Albert Gonzalez Carding Organization

F. THE HOMELAND SECURITY CONNECTION

The examples in the previous section illustrate that theft of card data from point-of-sale systems is truly an international problem. State and local law enforcement agencies are generally limited in their reach against these international crime rings, mainly due to jurisdictional restrictions, but also due to funding and other resource problems. State and local police departments can and do play a critical role in arresting the end users or “mules” of counterfeit credit, debit, and ATM cards. In fact, the dismantling of the Shadow Crew carding organization began largely when a New York City Police detective arrested Albert Gonzalez in the act of “cashing out,” or using counterfeit ATM cards encoded with stolen data (Verini, 2010).

Furthermore, the significant number of compromised card accounts, coupled with billions of dollars in fraud losses and other expenses, poses a serious threat to the health of the United States economy, and is therefore a homeland security problem. Table 1 shows a list of some of the major card breaches in recent U.S. history Krebs, 2013; FBI, 2009; US v. Gonzalez, 2010; Cratty, 2012; Pepitone, 2014). These breaches alone yielded hackers almost 270 million credit and debit card numbers, with an estimated fraud loss of almost $135 billion.

Table 1. Payment Card and Fraud Losses for Major Breaches

Victim	Number of Payment Cards Compromised	Estimated Fraud Loss
Target Stores	40 million	$20 billion*
RBS World Pay	N/A	$9 million
Hannaford Grocery	4.2 million	$2 million
DSW (online shoe store)	1 million	$500 million*
Dave & Buster’s	240,000	$3 million
TJ Maxx/Marshall’s	94 million	$47 billion*
Heartland Payment Systems	130 million	$65 billion*

* Exact fraud loss amounts not available; figures derived from the number of payment cards compromised with an average fraud loss of $500, per the United States Sentencing Commission

Criminals obtain the majority of their stolen card numbers by hacking into point-of-sale systems. In fact, of the three largest card data breaches in U.S. history, two were the result of point-of-sale compromises (US v. Gonzalez, 2008; US v. Gonzalez, 2009; Krebs, 2014, February 12):

Table 2. Three Largest Payment-card Breaches and Primary Method of Compromise

Victim	Primary Method of Compromise
TJ Maxx/Marshall’s	Point-of-sale system compromised via cracked WEP keys on 802.11 wireless system
Heartland Payment System	SQL Injection against Website
Target Stores	Point-of-sale system compromised after hackers broke into a trusted third party system and made their way to Target’s point-of-sale system

While criminals do obtain stolen card data through various hacking methods, including SQL injection, the majority of compromised accounts and the majority of individual intrusions involve attacks against retail point-of-sale systems. As point-of-sale systems yield the greatest fraud losses and therefore impact on the U.S. economy, any efforts toward mitigating the homeland security problem of trans-national carding organizations must begin with reducing the frequency and impact of intrusions against point-of-sale systems.

IV. A SURVEY OF CRIMINAL INVESTIGATIONS OF POINT-OF-SALE SYSTEM INTRUSIONS

A. NATURE AND PURPOSE OF RESEARCH

To gain insight into the mechanics of criminal point-of-sale intrusions, we conducted forty-two criminal investigations of point-of-sale breaches by the United States Secret Service. We reviewed all point-of-sale cases opened from January 2013 through January 2014. In general, Secret Service agents begin a point-of-sale investigation following one of two conditions:

- A bank or other financial institution notifies a Secret Service field office that a retail establishment appears to be a "common point of compromise." When fraudulent purchases appear on a legitimate cardholder's account, financial institute fraud investigators look for common locations where the legitimate cardholder used the payment card. For example, if Mom's Bank received complaints of fraudulent purchases from twelve different customers, and all twelve made a purchase at Dad's Café, then Dad's Café is the common point of compromise, and the nearest Secret Service office to Dad's café will dispatch an agent to investigate. Based on results of our research, this is the most common method.
- Secret Service agents investigating criminal carding organizations will learn about a specific point-of-sale breach through confidential informants or undercover methods.

For our research, we read investigative and forensic reports related to point-of-sale investigations. For each case, we sent a survey to the lead investigative agent to gather specific information about the nature of the intrusion.

We attempted to gather the following information:

- What was the specific manner of intrusion into the point-of-sale system?
- What was the duration of the compromise?
- How many cards were compromised, or what was the fraud loss as a result of the intrusion?
- Did the attackers use malicious code, and if so, what type of code did they use?

How did the victims (i.e., the businesses who used the point-of-sale system) learn of the intrusion?

We collected the data with the following larger questions in mind:

- Are there recurring types of malicious code used with point-of-sale system intrusions?
- How prevalent are zero-day malicious code infections?
- What is the average duration of a point-of-sale compromise?
- What is the average fraud loss or number of cards compromised?
- What are the primary attack or infiltration methods?
- How do the hackers exfiltrate stolen card data from compromised point-of-sale systems?

B. SURVEY METHODS

We identified forty-two new cases concerning point-of-sale system intrusions for the period of January 2013 through January 2014 by reviewing all network-intrusion investigations by the Secret Service specifically focused on point-of-sale systems. We sent a survey to the case agent in charge of each of the forty-two point-of-sale system investigations. Of the forty-two surveys we submitted, we received responses from forty-one. The survey included seven questions related to the nature of the point-of-sale system compromise, including length of intrusion, method of intrusion, method of card exfiltration, and the method by which the intrusion was discovered.

C. RESULTS

The table in the appendix summarizes each case. In some instances, specific data was not provided such as duration of the intrusion or specific malicious code used due to one of the following:

- The business owner or point-of-sale system vendor may have performed a system clean-up or completely rebuilt the system before law enforcement or third-party forensic vendors had an opportunity to perform forensic analysis.

- During the investigation the case agent (i.e., the Secret Service agent leading the criminal investigation) presented a summary of the case, including fraud loss, identities of suspects, etc., to a federal prosecutor. If the federal prosecutor declined to prosecute, the Secret Service ceased any further investigation or forensic analysis.
- In a small number of cases the business owner may have hired a private forensic firm to conduct a private investigation and implement security improvements. The third-party analyses do not always address the specific research questions we pursued.
- Some investigations were in the early phases and complete data was not yet available

The table in the appendix provides a summary of each criminal investigation undertaken by the United States Secret Service of point-of-sale system intrusions from January 2013 through January 2014. The table reveals some interesting statistical trends:

- The most common entry point into point-of-sale systems was through poorly secured remote-desktop environments. Other security risks were having no firewall, having missing or out-of-date anti-virus protection, and using point-of-sale system terminals for personal Internet activities.
- The most common form of malicious code was Perfect Keylogger for hard-disk-based keystroke loggers, and the “sr.exe” and “searcher.dll” pair for random-access memory-based “scrapers.” A “memory scraper” or “RAM scraper” is malicious code that monitors specific point-of-sale processes in random-access memory to catch payment-card data when it is temporarily unencrypted as it transits certain processes in memory (Kotov, 2014).
- In most cases, banks or other financial institutions identified the victim business by recognizing the “common point of compromise.”
- In some instances victims were identified through other Secret Service investigations. For example, a Secret Service agent may arrest a suspect in a point-of-sale intrusion case who admits to hacking into other, unreported point-of-sale systems.
- In no cases did the victims first learn about the intrusions on their own.

- For cases where the duration of the intrusion is known, its average length was 6.3 months.
- The total number of stolen cards identified to date is 2,498,956 for forty-two criminal cases. If we use the U.S. Sentencing Commission standard fraud loss per card of $500.00, then the potential fraud loss for these forty-two investigations alone is $1.2 billion. The number of compromised cards will likely grow as financial institutions complete their assessments.

This survey revealed that point-of-sale system intrusions were not sophisticated, because they did not need to be. In most cases, hackers breach the point-of-sale system by scanning for standard port numbers associated with remote desktop environment products or services. Then the hacker generally tries default passwords or easy-to-guess passwords.

V. FORENSIC INDICATORS OF POINT OF SALE SYSTEM ATTACKS

A. POINT-OF-SALE SYSTEM ATTACK CHARACTERISTICS

Point-of-sale system intrusion methods reflect the gamut of the larger world of network intrusions and include a mix of physical attacks, Web-based attacks, and network attacks. A brief survey of some of the largest point-of-sale system intrusions illustrates this spectrum (Berg, Freeman, & Schneider, 2008; Krebs, 2011; Krebs, 2014, February 06; US v. Gonzalez, 2009):

Table 3: Intrusion Methods for Major Point-of-sale Intrusions

Victim	Initial method of intrusion
TJ Maxx chain	Cracked WEP Wi-Fi password
Michael’s Craft Stores	Physical tampering of POS terminals
Target Department Store chain	Compromised 3rd party credentials
Hannaford Supermarket chain	SQL Injection

While criminals apply a variety of methods against larger retail corporations, they more often attack smaller retail establishments by focusing on remote-desktop (remote-access) connections. The statistical data collected in Chapter IV show that out of thirty cases with a known or suspected method of compromise, sixteen involved remote desktop software. In a white paper for the 2010 Black Hat USA conference, researchers from the security and forensics company Trustwave called exploitation of point-of-sale remote access “the easy way” (Percoco and Ilyas, 2010). Trustwave’s *2013 Global Security Report* identified remote desktop exploitation as the cause of 47% of all network intrusions that company investigated (Trustwave, 2013).

Many small and medium-size retail establishments use simple remote-access software (e.g., PC Anywhere, GoToMyPC, LogMeIn, or Microsoft Remote Desktop) to allow point-of-sale technicians and restaurant managers to remotely access the system at any time. If a bar or restaurant experiences point-of-sale system troubles during a busy Saturday night, the establishment wants the system fixed immediately, and the point-of-sale technician wants to avoid a possibly long drive to the restaurant. Thus, there is sound business logic for remote access. Criminals have learned, however, that many businesses use remote-access products with weak passwords. Therefore, criminals merely need to run a port-scan tool such as Nmap against potential point-of-sale IP addresses, looking for standard port numbers for remote access products. For example, Microsoft's Remote Desktop Protocol runs on TCP port 3389, and PC Anywhere operates on TCP port 5631 or 5632. Once an attacker has collected a list of potential targets, the attacker can try a list of common login names and passwords. In some cases, point-of-sale system components were left configured with standard login name and password combinations (e.g., user name "aloha," password "aloha"), which exacerbated the problem (Trustwave, 2014).

Once criminals have entered the point-of-sale network, they usually install malicious code designed to capture payment-card data. In general, this malicious code is either traditional keylogger software (e.g., Perfect Keylogger) or random-access memory (RAM) scrapers. Keylogging software monitors input sources such as keyboards and card readers. Keylogging software such as Perfect Keylogger collects captured card data into a log file. The criminals may retrieve the log file manually (using the original intrusion method, often a poorly-secured remote-access application) or establish a file transfer protocol (FTP) or simple mail transfer protocol (SMTP) service to exfiltrate data from the compromised system. Attackers can configure the SMTP or FTP service to periodically export a payment-card log file to an external server or Web mail account.

Malware scrapers are currently the more common method of capturing card track data (Trustwave & USSS, 2012). When an employee swipes a card, the track data is briefly held in memory before the point-of-sale application encrypts it. Memory scrapers monitor specific buffers in memory known to be associated with specific point-of-sale processes. When the malicious code identifies new payment-card data, it is copied to a log file on the hard drive of the infected point-of-sale machine. Depending on the specific memory scraper tool being used, the scraper may perform additional actions on the collected data, such as parsing and encryption. Criminals can then retrieve the collected card data manually, repeating the initial intrusion methods (Trustwave, 2014).

B. A FORENSIC CASE STUDY

In a typical point-of-sale system implementation, employees swipe cards at one or more point-of-sale terminals. The track data is sent to a buffer in memory, either on the terminals themselves or at the back-of-house server (Trustwave, 2014; Trustwave, 2010). The point-of-sale system software reads the card data from the memory buffer and encrypts the cardholder data before it is sent to a financial institution for approval. Memory scrapers target cardholder data in the brief instant that it is unencrypted in the memory buffer.

To provide insight into potential forensic evidence from a criminal compromise of a point-of-sale system, we examined a back-of-house server from a victim restaurant. The compromised machine ran Microsoft Windows XP Service Pack 2 and a standard copy of Aloha Manager/EDC point-of-sale software, along with a copy of Symantec’s PCAnywhere to support remote access. The built-in Windows firewall was disabled, as were Windows Automatic Updates for system security patches.

For this server, we performed the following forensic steps:

1. We began with a “clean” Universal Serial Bus thumb drive. The drive was formatted with the NTFS file system to eliminate possible storage problems (e.g., file size and file name length) with the FAT 32 file system.

2. On the thumb drive we installed a “known good” copy of cmd.exe taken from a different computer with a fresh installation of Microsoft Windows.

3. We added a copy of the tool “Dumpit” from Moonsols to collect a copy of the target system’s random access memory (RAM). As a backup tool, we added a copy of Access Data’s FTK Imager Lite.

4. On the live (compromised) system, we inserted the thumb drive. After it mounted, we navigated to the drive letter of the thumb drive and ran the program cmd.exe.

5. At the Windows Command Line Interface (CLI), we collected volatile and system information via the following commands:

- F:\ ipconfig /all >>collection.txt
- F:\ natstat –ano >>collection.txt
- F:\ whoami >>collection.txt
- F:\ systeminfo >>collection.txt
- F:\ net user >>collection.txt
- F:\net accounts >>collection.txt
- F:\openfiles >>collection.txt
- F:\taskist /v >>collection.txt
- F:\wmic process list full >>collection.txt
- F:\net start >>collection.txt
- F:\tasklist /svc >>collection.txt
- F:\schtasks >>collection.txt
- F:\wmic startup list full >>collection.txt
- F:\ wmic useraccount where name=’edc’ get sid

The last command collected the system-identification value for the current logged-on user. This information is necessary to manually copy the user’s ntuser.dat file.

6. We ran the tool Dumpit from Moonsols from the command line, which copied the contents of the live system’s random-access memory into a dump file in the .raw format.

7. We manually copied the Windows Registry hive files with:

- F:\ reg save HKLM\SAM f:\regsamdump
- F:\ reg save HKLM\SYSTEM f:\regsystemdump
- F:\ reg save HKLM\SECURITY f:\regsecuritydump
- F:\ reg save HKLM\SOFTWARE f:\regsoftwaredump
- F:\ reg save hku\{user’s SID value} f:\ntuserdump.dat

8. We manually copied the Windows Event Logs using “copy *.wev f:\.”

9. We analyzed the gathered information with a variety of forensic tools, including:

- ***Bulk Data Extractor :*** Used for parsing useful strings (e.g., email addresses, Internet Protocol addresses) out of source, such as our memory dump file
- ***Strings*** : Used for pulling clear text strings out of a source, including formatted files
- ***Redline*** : Used for analyzing running processes and looking for indications of malicious code and rootkit infections
- ***RegRipper*** : Used to parse data from Windows Registry hives, including installed software, mounted hardware, entries in the Windows Prefetch file, and more.

- ***Volatility*** : Used to extract specific information such as data on running processes from memory-dump files. Volatility is built on a modular framework, which allows an examiner to choose specific plug-ins.
- ***YARU*** : Used for exploring imported Windows Registry hives in the native directory structure
- ***Event Log Explorer*** : Used for importing Windows Event Logs. Although the native Windows Event Viewer works well for this task, the Event Log Explorer tool offers more export options and can concatenate multiple Windows event logs into one file.

In the case of the compromised back-of-house server, forensic analysis revealed that criminals installed a three-part memory scraper tool on the server. The loader (controller) file rpcsrv.exe appears on a security alert of point-of-sale malicious code published by Visa, Inc. in 2009 (Visa, 2009), though the other files were not recognized.

The loader functioned as the malicious-code installer. It added a service for persistence, pointing to itself, and also loaded the other two files, one for parsing card strings in memory, and the other for data aggregation. After running the Strings tool against this file, the output revealed the two files this controller file was set to begin:

```
start /min algsvc.exe

start /min rdpsvc.exe
```

The second component was the actual memory-scraper tool. Memory scrapers are generally written to monitor specific point-of-sale executable files that process card track data. In the case of the infected back-of-house server, this machine ran Aloha’s EDC (Electronic Draft Capture) software for processing swiped card data. The memory scraping tool, algsvc.exe, monitors the legitimate

Aloha process (edcsvr.exe) in memory for credit card strings. An analysis of the memory scraper with the Strings tool shows specific references to edcsvr.exe.

The third component was a data-aggregation tool, rdpsvc.exe. It monitored data collected from the memory scraper and parsed card data. This data was then obfuscated and sent to dump files, which the criminals would retrieve manually.

C. SAMPLE FORENSIC INDICATORS OF POINT-OF-SALE SYSTEM INTRUSIONS

Non-volatile evidence may be collected via several techniques, including full disk-drive imaging with a write-blocking mechanism and imaging software, or through the collection of specific files or directories. In some instances an establishment is unable or unwilling to take its point-of-sale system offline for traditional disk imaging in which case non-volatile information can be collected directly from the machine.

Nonvolatile evidence includes persistent malicious code, Windows Registry keys, cache files, and log files. Malicious code in the form of keyloggers, especially common applications like Perfect Keylogger, will likely generate positive hits with anti-virus products. Point-of-sale specific malicious code may not be included in standard anti-virus signature lists, but Web resources do provide MD5 checksum values and Windows Registry key values for some malware scrapers (Visa, 2009; Trustwave, 2010; iSight, 2014; Wilson, Loftus, & Bing, 2013; Higgins, 2014).

For example, the security research company iSight published a list of non-volatile forensic indicators for the Kaptoxa point-of-sale malicious code set, which many believe was used in the Target department store intrusion (iSight, 2014; Krebs, January 2014). This list includes additions and modifications of fifteen Windows Registry keys (e.g., HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_POSWDS\0000\Control) and eighteen malicious code files that may be present in a Kaptoxa-infected point-of-sale system including name, extension, size, and four different hash values for each malicious file.

Volatile evidence is obtained by deploying specific data collection tools on the live machine. Although the use of these tools on a live device will leave evidence that an examiner used such tools (for example, in the Windows Registry key HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU) (Carvey, 2011), most live-response collection tools and methods leave a minimal footprint.

Volatile evidence may include running processes (hidden or open), suspicious network ports, volatile Windows Registry key values, temporary files, and memory-only malicious-code activity. Examiners may have prior information that enables them to focus on certain suspicious network ports or running processes. For the case study of the server, we know that the controller file loaded the memory-scraper program (algsvc.exe) and the card data parsing and aggregation program (rdpsvc.exe), both of which ran as normal (i.e., non-hidden) processes.

Network evidence can be useful to learn how stolen data exited the impacted network, as well as its destination. In some instances, for example zero-day exploits or highly stealthy techniques, network forensics may be the best option for discovering the outbound export of sensitive data. Indeed, when Google fell victim to an Advanced Persistent Threat (also known as an Operation Aurora attack) intrusion in 2010, Google’s incident-response team relied on Domain Name Service logs to piece together the nature of the attack (Westervelt, 2010).

Network forensic evidence is also useful in an investigation, and can come from log files (Domain Name Service, mail, Web, Dynamic Host Configuration Protocol, etc.) or by capturing network packets in real time. For the latter, the investigator can use a small network tap, a span port on a network switch, or a packet-capture tool such as Windump or Wireshark, although these generally require installation of new software which may violate the principle of making as few changes to the original evidence as possible. Capturing network packets in real time can be challenging, as the resulting capture files can grow very quickly. Nevertheless, running packet capture tools on traffic of a suspected infected machine may be the best option for determining the methods and destinations of outbound compromised data. As an example, the Arbor SERT revealed the following signatures from the recent Dexter point-of-sale malicious code (Wilson, Loftus, & Bing, 2013):

- GET /hint/chck.php HTTP/1.1
- Host: rome0[.]biz
- Accept: text/html, */*
- Accept-Encoding: identity
- User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; SLCC!
- Hxxp://rome0.biz/hint/cx.php

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS FOR PREVENTING POINT-OF-SALE INTRUSIONS

A. TECHNICAL SECURITY RECOMMENDATIONS

Information gathered from criminal investigations of point-of-sale system intrusions and from trend reports from Trustwave demonstrate that criminals often use predictable patterns of attack behavior along with easily identifiable malicious code. Poorly secured remote access is perhaps the most common entry method for criminals, and we recommend that retailers pay particularly close attention to improving it.

1. Secure remote access capabilities

If remote access between point-of-sale vendor technicians and the point-of-sale system is a necessary evil, then the point-of-sale system operators must operate it as securely as possible. We offer the following recommendations:

A. Avoid if possible remote-access products and services such as PCAnywhere, GoToMyPC, Microsoft RDP, LogMeIn, etc. Point-of-sale system operators can install an effective yet inexpensive hardware firewall with virtual private networking capabilities, such as the Cisco ASA 5510, sold by a variety of vendors for under $400.

B. If commercial remote access products are unavoidable, point-of-sale operators (i.e., the restaurant, hotel, or store) should establish good passwords necessary to access the system. Do not allow point-of-sale system vendors to establish user names and passwords. Users should follow best practices for length, expiration, and complexity. Users can check the strength of a given password from a variety of password checking Web sites, including www.passwordmeter.com.

C. If commercial remote-access products are unavoidable, point-of-sale operators should consider enabling the remote access service only when it is needed. If an off-site employee or point-of-sale technician requires remote access, require that they call in to request its enablement. Point-of-sale operators should be able to disable the remote-access product when not in use by suspension or shut-off functions within the application, or by stopping the running process at the command line or within Windows Task Manager.

2. Use an effective anti-virus product

Anti-virus products may not be effective against some types of malicious code that only attacks point-of-sale systems (Trustwave, 2014). Nevertheless, anti-virus products are still effective in identifying popular keystroke logging tools, such as Perfect Keylogger. Point-of-sale system users should use an anti-virus product, configure it to receive automatic updates, and run automatic scans.

3. Use a firewall

In addition to using a hardware firewall to protect the point-of-sale system's network, operators should use a software firewall on each terminal and the back-of-house server. These add an additional layer of security and another opportunity for log file activity. Microsoft Windows includes a built-in firewall with the Windows operating system.

4. Restrict point-of-sale nodes to specific business use

Point-of-sale system operators should forbid employees from using point-of-sale system terminals and back-of-house servers for other Internet activities such as visiting Web sites, checking e-mail, etc. All nodes on the point-of-sale system should be restricted to the business functions of processing sales and card information to limit opportunities for malicious access.

5. Operate point-of-sale system nodes with least privileges

Operations of point-of-sale terminals and back-of-house servers should use minimal privileges (i.e., non-administrative accounts). Operators should disable any unnecessary accounts (e.g., guest) and ensure all accounts follow information security best practices for password use (length, expiration, complexity).

6. Harden the operating system of point-of-sale system nodes

Point-of-sale system operators should strengthen the security of the underlying operating systems of point-of-sale nodes. They should consider security configuration guides from the National Institute of Standards and Technology. Specific suggestions include enabling automatic updates and disabling unnecessary applications and services.

B. A POINT-OF-SALE-SYSTEM SECURITY AWARENESS CAMPAIGN

Several organizations have published advisories and security configuration checklists for point-of-sale terminals. For example, in January 2014 the United States Computer Emergency Readiness Team (US-CERT) published a two-page document, “Malware Targeting Point of Sale Systems” (US-CERT, 2014). This advisory provides a brief overview of point-of-sale systems, the nature of point-of-sale system compromises, and a brief bulleted list of recommended security steps. Visa released a slightly more technical report, “Retail Merchants Targeted by Memory-Parsing Malware–Update” (Visa, 2014). This document provides a more specific two-page list of point-of-sale system security steps, but Visa also includes without explanation a two-page list of point-of-sale system malicious code file names and MD5 hash values. Although this information is very helpful to investigators, it is doubtful that most small and medium size point-of-sale operators will know what to do with MD5 hash values.

The Department of Homeland Security can help lead a public awareness campaign for the improvement of point-of-sale system security. This program clearly meets two key objectives of the Department, as specified in the *Quadrennial Homeland Security Review Report* (DHS, 2010): (1) prevent cyber crime and other malicious uses of cyberspace, and (2) enhance public awareness.

As a precedent, the United States Secret Service, a component of the Department of Homeland Security, has for several years managed a successful international public awareness campaign concerning genuine currency. This awareness campaign uses a multi-level approach to public education, ranging from colorful flyers and posters for general information to detailed Web sites, seminars, and brochures for banks, retailers, and others who handle large amounts of currency. A point-of-sale security public awareness campaign could follow a similar layered approach. The first layer can feature easy-to-follow flyers, posters, and brochures that illustrate basic elements of point-of-sale system security. These items should use graphics and catchy phrases that will capture the attention of average point-of-sale system users. Middle layers can provide more specific “checklist” style steps toward improving point-of-sale system security, most likely in document format. Advanced layers can provide more technical security improvement procedures, including specific steps for different vendors of point-of-sale systems.

APPENDIX

Summary of United States Secret Service point-of-sale system intrusion investigations (RDE = Remote Desktop Environment)

Case #	Possible Intrusion Method	Malware and/or Hacker Tools Used	Victim Notified by:	Fraud Loss or Number of Payment Cards Stolen: Category	Approx. Duration of Intrusion	Notes
1	Vulnerable RDE	Unspecified keylogger and remote Trojan	N/A	F	Unknown	
2	Vulnerable RDE	Sr.exe; searcher.dll; run.exe	Bank(s)	A	Unknown	
3	Unknown but RDE in use	Unknown	Bank(s)	D	3 months	Victim did partial system repair prior to law enforcement contact
4	RDE with weak password; no firewall	Sr.exe; searcher.dll; run.exe	Bank(s)	A	3 months	
5	Vulnerable RDE	Sr.exe; searcher.dll	Bank(s)	A	1 month	
6	Unknown	Sqlmgmt.exe; Rptsvc32.exe; sppt32.exe	Bank(s)	Unknown	2 months	
7	RDE with default passwords	Perfect Keylogger	Bank(s)	A	5+ months	
8	Weak login password	Suidshell malware	Bank(s)	B	5 months	Rare *nix POS system
9	POS terminals used for personal Internet activities	Perfect Keylogger; wuauclt.exe	Data from another criminal case	A	8 months	

10	Unknown	Spyeare.HidetoolsSpy	Data from another criminal case	A	2 months	
11	Unknown	Unspecified RAM dumper	Bank(s)	A	14 months	
12	Unknown	Unspecified Trojan (hidden as “scvhost.exe”; note the unusual spelling)	Data from another criminal case	A	6 months	
13	Unknown	Spoolsw.exe	Bank(s)	Unknown	Unknown	
14	Anti-virus 2 years out of date; POS terminals used for personal Internet use	Two possible: “msseces.exe” and “ctfmon.exe”	Bank(s)	A	5 months	
15	No firewall; no anti-virus	Trojan.vundo	Bank(s)	D	Unknown	
16	Vulnerable RDE	Perfect Keylogger	Unknown	A	5 weeks	
17	Vulnerable RDE	Unspecified RAM dumper	Unknown	Unknown	Unknown	
18	Weak passwords	“Wnhelp.exe”; “Mmon.exe” (the latter specifically captures credit card track data); SAMInside password cracker found on system	Bank(s)	E	5 weeks	
19	Blank admin password	“Sr.exe” and “Searcher.dll”	Bank(s)	Unknown	27 months	
20		Survey not returned				
21	Weak passwords	“Sr.exe” and “Searcher.dll”	Unknown	Unknown	Unknown	
22	Possible infection due to use of POS system for personal Internet use	“Downloadermstdc.exe”; possibly 61 pieces of malicious code across multiple franchise locations	Bank(s)	C	3 months	

23	POS vendor’s RDE account was compromised	“Trojan.agent.s.z”; “Aluroot-b”	Bank(s)	E	Unknown	
24	Evidence that victim was phished	Unspecified malicious code	Bank(s)	D	Unknown	
25	Victim’s card processing company was penetrated	Evidence of malicious command shell access found during forensic work, but no specific malware or hacking tools found to date	Bank(s)	F	1 month	
26	3 different RDE products found on POS system; owner only knew of one	Unknown	Bank(s)	D	Unknown	
27	Vulnerable RDE	Unknown	Bank(s)	D	Unknown	
28	Vulnerable RDE	2 Keyloggers: “hkcmd.exe” and “winupd.exe”; 2 RAM scrapers: “sr.exe”/”searcher.dll” and “mmon.exe”	Private Forensic Company	A	9 months	
29	Unknown	Perfect Keylogger	Bank(s)	A,D	c. 4months	
30	No firewall; vulnerable RDE	2 Keyloggers: “Perfect Keylogger” and “Ardamax”	Bank(s)	3,600 cards	20 months	
31	No firewall; vulnerable RDE	Perfect Keylogger	Data from another criminal case	A	17 months	

32	Unknown	Perfect Keylogger	Data from another criminal case	A	8 months	
33	Unknown	“Ardamax” keylogger and “Infostealer.bancos Trojan	Data from another criminal case	A	4 months	
34	Unknown	Zero day or custom Keylogger	Data from another criminal case	A	Unknown	
35	Vulnerable RDE	“Ardamax” keylogger	Data from another criminal case	Unknown	16 months	Criminal intent may be more focused on identity theft than payment card fraud
36	Vulnerable RDE	Unknown but “Ardamax” keylogger suspected	Data from another criminal case	Unknown	1 month	Criminal intent may be more focused on identity theft than payment card fraud
37	Unknown	Zero day or custom keylogger	TBD	TBD	4 months	
38	Unknown	“Alghlp.exe”; “Ntmpsvc.exe”; “Mcservice.exe”	Bank(s)	A	3 months	
39	Business chain; most franchises used RDE	All victim franchises had some combination of “Sr.exe”/”Searcher.dll”; “Rdasrv.exe”; and “Cardrecon_v1.14.17_cracked.exe” on their systems	TBD	B	TBD	

40	Unknown	“Trojan 2-bot” and unspecified keylogger	Bank(s)	D	Unknown but fraud attempts lasted for 2 months	POS vendor did some clean up before law enforcement involvement
41	Vulnerable RDE	“Sr.exe” and “Searcher.dll”	Bank(s)	A	1 month	
42	Vulnerable RDE	“Zbot” (aka Zeus Trojan); “Alina” virus (RAM scraper)	Bank(s)	C	1-3 months	

Note that some entries with “unknown” data are recent cases in which forensic or investigative data may be forthcoming. In others, a federal prosecutor declined further consideration of the case, causing law enforcement to cease forensic and investigative activities.

“Vulnerable RDE” means the victim used a default installation of a popular remote desktop environment, usually PC Anywhere, GoToMyPC, LogMeIn, or Microsoft Remote Desktop. In some cases the victim (business) was not aware of the presence of the remote desktop environment; in many cases the remote desktop environment used weak passwords.

Key for “Fraud Loss or Number of Payment Cards Stolen” column:

A – Fewer than 10,000 payment cards stolen
B – 10,001 – 25,000 payment cards stolen
C – More than 25,000 payment cards stolen
D – Fraud loss less than $50,000
E – Fraud loss between $50,000 and $250,000
F – Fraud loss greater than $250,000

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Acohido, B. (2009, January 20). Hackers breach heartland payment credit card system. Retrieved from USA Today website: http://usatoday30.usatoday.com/money/perfi/credit/2009-01-20-heartland-credit-card-security-breach_N.htm

Associated Press. (2014, February 04). *Target data breach pits banks against retailers*. Retrieved from http://bigstory.ap.org/article/target-data-breach-pits-banks-against-retailers

Berg, G., Freeman, M., & Schneider, K. (2008, August). Analyzing the TJ Maxx data security fiasco. *The CPA Journal Online*. Retrieved from http://www.nysscpa.org/cpajournal/2008/808/essentials/p34.htm

Beverly, R., Garfinkel, S., Cardwell, G. (2011). Forensic carving of network packets and associated data structures. *Digital Investigation*, Volume 8 pp. S78-S89

Bhattacharjee, Y. (2011, January 31). *How a remote town in Romania has become cybercrime central*. Retrieved from Wired.com website: http://www.wired.com/2011/01/ff_hackerville_romania/

Bowles, S., Cuthbert, B., & Stewart, W. (2005, September 22). *Typical attack techniques for compromising point of sale PIN entry devices*. EWA-Canada. Retrieved from http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/physec/papers/physecpaper04.pdf

Bran, M. (2013, January 07). In Romania, a quiet city has become the global hub for hackers and online crooks. Retrieved from Worldcrunch.com website: http://www.worldcrunch.com/tech-science/in-romania-a-quiet-city-has-become-the-global-hub-for-hackers-and-online-crooks/hacking-hacker-romania-pirate-scam-internet-website/c4s10532/

Carvey, H. (2012). *Windows forensic analysis toolkit,* Third Edition. Waltham, MA: Elsevier.

Carvey, H. (2011). *Windows registry forensics: Advanced digital forensic analysis of the windows registry*. Burlington, MA: Elsevier.

Chappell, L. (2012). *Wireshark network analysis*, Second Edition. San Jose: Protocol Analysis Institute.

Cratty, C. (2012, July 18). *Hacker Gets 7 Years in thefts of more than 240,000 credit card numbers*. Retrieved from Cnn.com website: http://www.cnn.com/2012/07/18/justice/credit-card-thefts/

Department of Homeland Security (DHS). (2010). Quadrennial Homeland Security review report. Washington, DC: Author. Retrieved from http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf

Department of Justice. (2013, September 04). *Two Romanian nationals sentenced to prison for scheme to steal payment card data*. Retrieved from http://www.justice.gov/opa/pr/2013/September/13-crm-987.html

Department of Justice. (2012, June 15). *Alleged International credit card trafficker "Badb" extradited from France to the United States*. Retrieved from http://www.justice.gov/opa/pr/2012/June/12-crm-767.html

Department of Justice. (2010, August 11). *Alleged international credit card trafficker arrested in France on U.S. charges related to sale of stolen card data*. Retrieved from http://www.justice.gov/opa/pr/2010/August/10-crm-921.html

D'Innocenzio, A. (2014, January 12). *Neiman Marcus latest chain to disclose credit card theft*. Retrieved from Boston Globe website: http://www.bostonglobe.com/news/nation/2014/01/12/neiman-marcus-latest-victim-security-breach/pZHhuxgM2Nnl5YtVQZHi6K/story.html

Douglas, Danielle. (2014, February 04). *Retailers to Congress: There's no end in sight for credit card breaches*. Retrieved from Washington Post website: http://www.washingtonpost.com/blogs/wonkblog/wp/2014/02/04/retailers-to-congress-theres-no-end-in-sight-for-credit-card-breaches/

Fazio, R. (n.d.) Statement on Target data breach. Retrieved from Faziomechnical.com website: http://faziomechanical.com/Target-Breach-Statement.pdf

Federal Bureau of Investigation. (2009, November 10). International effort defeats major hacking ring. Retrieved from http://www.fbi.gov/atlanta/press-releases/2009/atl111009.htm

FICO. (2010, October). Card compromises- new risks and best practices. Retrieved from http://www.fico.com/en/wp-content/secure_upload/45_Insights_Card_Compromises_2713WP.pdf

Finkle, J., & Hosenball, M. (2014, January 12). *Exclusive: More well-known U.S. retailers victims of cyber attacks- sources*. Retrieved from Reuters.com website: http://www.reuters.com/article/2014/01/12/us-target-databreach-retailers-idUSBREA0B01720140112

Fraud and related activity in connection with computers, 18 U.S. Code § 1030 (2008). Retrieved from http://www.law.cornell.edu/uscode/text/18/1030?qt-us_code_tabs=0#qt-us_code_tabs

Hans, G.S. (2014, February 07). *Target and Neiman Marcus testify on data breach- but what reforms will result?* Retrieved from Center for Democracy and Technology website: https://www.cdt.org/blogs/gs-hans/0702target-and-neiman-marcus-testify-data-breach-%E2%80%93-what-reforms-will-result

Hejazi, S.M., Talhi, C., & Debbabi, M. extraction of forensically sensitive information from Windows physical memory. *Digital Investigation*, 6, S121-S131.

Hizver, J. and Chiueh, T. (2012). An Introspection-Based Memory Scraper Attack against Virtualized Point of Sale Systems. *Lecture Notes in Computer Science*, vol. 7126. Pp 55-69

iSight Partners. (2014, January 14). Kaptoxa point-of-sale compromise. Retrieved from Securitycurrent.com website: http://www.securitycurrent.com/resources/files/KAPTOXA-Point-of-Sale-Compromise.pdf

Katz, K. (2014, January 22). *To our loyal Neiman Marcus group customers.* Retrieved from Neiman Marcus.com website: http://www.neimanmarcus.com/NM/Security-Info/cat49570732/c.cat?icid=topPromo_hmpg_ticker_SecurityInfo_0114

Krebs, B. (2014, February 12). *Email attack on vendor set up breach at Target*. Retrieved from KrebsOnSecurity website: http://krebsonsecurity.com/2014/02/

Krebs, B. (2014, February 06). *Target hackers broke in via HVAC company*. Retrieved from KrebsOnSecurity website: http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company

Krebs, B. (2014, January 10). *Hackers steal card data from Nieman-Marcus*. Retrieved from KrebsOnSecurity website: http://krebsonsecurity.com/2014/01/page/2/

Krebs, B. (2013, December 18). *Sources: Target investigating data breach*. Retrieved from KrebsOnSecurity website: http://krebsonsecurity.com/2013/12/

Krebs, B. (2011, May 11). *Breach at Michaels stores extends nationwide*. Retrieved from KrebsOnSecurity website: http://krebsonsecurity.com/2011/05/breach-at-michaels-stores-extends-nationwide/

Lyon, G. (2008) *NMAP network scanning: The official NMAP project guide to network discovery and security scanning*. Sunnyvale, CA: Insecure.Com LLC.

Odobescu, V. (2014, January 13). *U.S. data thefts Turn spotlight on Romania*. Retrieved from USAToday.com website: http://www.usatoday.com/story/news/world/2014/01/13/credit-card-hacking-romania/4456491/

Pepitone, J. (2014, January 12). *5 of the biggest ever credit card hacks*. Retrieved from Cnn.com website: http://money.cnn.com/gallery/technology/security/2013/12/19/biggest-credit-card-hacks/3.html

Percoco, N., Ilyas, J. (2010, July 01). *Malware freakshow 2010*. Retrieved from Blackhat.com website: https://media.blackhat.com/bh-us-10/presentations/Percoco_Ilyas/BlackHat-USA-2010-Percoco-MalwareFreakshow2010-slides.pdf

Percoco, N., Sheppard, C., and Ilyas, J. (n.d.). *Evolution of malware: Targeting credit card data in memory*. Retrieved from Trustwave website: https://www.trustwave.com/downloads.whitepapers/Trustwave_WP_Evolution_of_Malware_.pdf

Percoco, N. et al. (2013). *Trustwave 2013 global security report*. Retrieved from Trustwave website: http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

Quick, Becky. (2014, January 12). Target CEO defends 4-day wait to disclose massive data hack. Retrieved from CNBC.com website: http://www.cnbc.com/id/101329300

Raff, Aviv. (2014, January 16). *PoS malware targeted Target*. Retrieved from Seculert website: http://www.seculert.com/blog/2014/01/pos-malware-targeted-target.html

Selyukh, A. (2014, February 11). *New hopes for U.S. data breach law collide with old reality*. Retrieved from Reuters.com website: http://www.reuters.com/article/2014/02/11/us-usa-security-congress-idUSBREA1A20O20140211

Target Corporation. (2013, December 19). *Target confirms unauthorized access to payment card data in U.S. stores*. Retrieved from http://pressroom.target.com/news/target-confirms-unauthorized-access-to-payment-card-data-in-u-s-stores

Target Corporation. (2013, December 20). A message from CEO Gregg Steinhafel about Target's payment card issues. Retrieved from Target.com website: https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca

Trustwave. (2014, March 10). *Combatting point-of-sale malware: White paper*. Retrieved from http://www2.trustwave.com/rs/trustwave/images/Special_Report_Combatting_Point_of_Sale_Malware.pdf

Trustwave. (2012). 2012 Payment card trends and risks for small merchants. Retrieved from https://www.trustwave.com/Resources/Library/Documents/2012-Payment-Card-Trends-and-Risks-for-Small-Merchants/

Trustwave. (2008). Forensics update: Trustwave's investigations of credit card compromises through October 2008. Previously available from https://www.trustwave.com/downloads/whitepapers/Trustwave_WP_Forensics_Update_Cases_through_October_2008.pdf

United States of Amercia v. Albert Gonzalez. (2010, March 18). United States District Court, District of Massachusetts. Retrieved from Wired.com website: http://www.wired.com/images_blogs/threatlevel/2010/03/gonzalez_gov_sent_memo.pdf

United States of America v. Albert Gonzalez, Hacker 1, and Hacker 2. (2009, August 17). United States District Court, District of New Jersey. Retrieved from http://www.wired.com/images_blogs/threatlevel/2009/08/gonzalez.pdf

United States of America v. Adrian-Tiberiu Oprea, Cezar Iulian Butu, Iulian Dolan, and Florin Radu. (2011, May 04). Case number Cr. No. 11-cr-64-01/04-SM. Retrieved from Wired.com website: http://www.wired.com/images_blogs/threatlevel/2011/12/Indictment_Romanian-POS-Hackers.pdf

United States of America v. Vladislav Anatolievich Horohorin. (2009, November 12). Case 1:09-cr-00305-ESH. Retrieved from http://www.wired.com/images_blogs/threatlevel/2010/08/BadB-Indictment-in-DC.pdf

United States Senate. (2014, March 26). *A "kill chain" analysis of the 2013 Target data breach.*" Retrieved from http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883

United States Sentencing Commission. (2013). *2013 Guidelines manual*. Washington, DC: Author. Retrieved from http://www.ussc.gov/Guidleines/2013_Guidelines/Manual_HTML/2b1_1.htm

Unknown author. (2010, August 12). *A BadB welcome cartoon*. Retrieved from YouTube website: http://www.youtube.com/watch?v=9y4iijOXGeg

US-CERT. (2014, January 02). *Malware targeting point of sale systems*. Retrieved from https://www.us-cert.gov/ncas/alerts/TA14-002A

Venter, S., Sheppard, C., & and Percoco, N. (2010, June). *POS memory parsing malware briefing: Attacks on kernel memory*. Retrieved from Trustwave website: http://Trustwave_SpiderLabs_Briefing_POS_Malware_Attacks_on_Kernel_Memory_June_2010-2.pdf

Verini, J. (2010, November 10). *The great cyberheist*. Retrieved from The New York Times website: http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?pagewanted=all&_r=0

Visa Inc. (2009, November 06). Visa data security alert: Targeted hospitality sector vulnerabilities. Retrieved from http://usa.visa.com/download/merchants/targeted-hospitality-sector-vulnerabilities-110609.pdf

Westervelt, R. (2010, June 17). How Google used DNS logs to investigate Aurora attacks. Previously retrieved from searchsecurity.com website: http://searchsecurity.techtarget.com/news/1514965/for-google-dns-log-analysis-essential-in-aurora-attack-investigation

Wilson, C., Loftus, D. & Bing, M. (2013, December 03). Dexter and Project Hook break the bank: Inside recent point-of-sale malware campaign activities. Retrieved from arbornetworks.com website:

http://www.arbornetworks.com/asert/wp-content/uploads/2013/12/Dexter-and-Project-Hook-Break-the-Bank.pdf

Zetter, K. (2010, August 11). *Alleged carder 'BadB' busted in France—Watch His Cartoon*. Retrieved from Wired.com website: http://www.wired.com/2010/08/Badb

Zetter, K. (2009, December 21). Albert Gonzalez enters guilty plea in Heartland, Hannaford Cases. Retrieved from Wired.com website: http://www.wired.com/2009/12/gonzalez-guilty-plea-heartland/

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California